Definition 2.11. An element $r \in R$ is called *nilpotent* if there exists $n > 0$ such that $r^n = 0$.

Example 2.12. (1) $0 \in R$ is nilpotent.
(2) $\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \in M_2(R)$ is nilpotent.
(3) If R is an integral domain, then

$$\begin{aligned} r^n = 0 &\Rightarrow r = 0 \text{ or } r^{n-1} = 0 \\ &\Rightarrow r = 0 \text{ or } (r = 0 \text{ or } r^{n-2} = 0) \\ &\Rightarrow \dots \Rightarrow r = 0, \end{aligned}$$

and so the only nilpotent element is 0.

Definition 2.13. An element $e \in R$ is called *idempotent* if $e^2 = e$.

Example 2.14. If R is unital, then for $1 \leq i \leq n$ the element $e_{ii} \in M_n(R)$ is idempotent.

Definition 2.14. Let K be a field. A *K-algebra* is a ring A which is also a K-vector space such that

- ring addition and vector space addition coincide, and
- $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $\lambda \in K$, $a, b \in A$.

Example 2.15. (1) K is a K-algebra. More generally, $K[X_1, \dots, X_n]$ is a K-algebra.
(2) If A is a K-algebra, then $M_n(A)$ is a K-algebra for any $n \geq 1$. Moreover, $U_n(A)$ and $L_n(A)$ are also K-algebras.
(3) If there is a subring $F \subseteq Z(R)$ such that F is a field, then R is an F-algebra.

Definition 2.16. Let R_i, $i=1,2,\dots$ be a family of rings. The <u>direct product</u> $R=\prod_i R_i = \times_i R_i$ is defined to be the set
$$R=\{(r_1,r_2,\dots) \mid r_i\in R_i\},$$
which is a ring under the operations
$$(r_1,r_2,\dots)+(s_1,s_2,\dots)=(r_1+s_1,r_2+s_2,\dots),$$
$$(r_1,r_2,\dots)\cdot(s_1,s_2,\dots)=(r_1s_1,r_2s_2,\dots),$$
for $(r_1,r_2,\dots),(s_1,s_2,\dots)\in R$.
The subset $S\subseteq R$ defined by
$$S=\{(r_1,r_2,\dots)\in R \mid r_i=0 \text{ for all but finitely many } i\}$$
is a subring of R called the <u>direct sum</u> and denoted by $S=\bigoplus_i R_i$.

Remark 2.17. Let $R_1,\dots,R_n$ be rings. Then
$$R_1\oplus\cdots\oplus R_n = R_1\times\cdots\times R_n.$$

Lemma 2.17. (1) Let $r\in R$. If there exists a unique $s\in R$ such that $rs=r$, then $sr=r$.
(2) Assume that there exists a unique $e\in R$ such that $re=r$ for all $r\in R$. Then $e=1_R$ is a multiplicative identity and R is unital.

Proof. (1) We have
$$r(s+sr-r)=rs+(rs)r-r^2=rs+rr-r^2=r+r^2-r^2=r$$
and so, by uniqueness of s, we conclude that $s+sr-r=s$, or $sr=r$.
(2) Let $r\in R$ and set $e'=e+er-r$. Then for all $x\in R$ we have
$$xe'=x(e+er-r)=xe+x(er)-xr=x+xr-xr=x$$
and so by assumption we conclude that $e'=e$

or $e+er-r=e$, or $er=r$. Hence $er=r$ $\forall r\in R$, and since $re=r$ $\forall r\in R$ by assumption, we conclude that $e=1_R$. $\square$

<u>Lemma 2.18.</u> Assume R is unital and let $r\in R\setminus\{0\}$. If there exists unique $s\in R$ with $rsr=r$, then $rs=1=sr$ and so r is invertible in R.

<u>Proof.</u> We have
$$r(s+sr-1)r = rsr+rsr^2-r^2 = r+r^2-r^2 = r,$$
and so by uniqueness of s we have $s+sr-1=s$ or $sr=1$. Similarly we get $rs=1$.

<u>Lemma 2.19.</u> Assume R is unital and let $r\in R$ have a right inverse. Then exactly one of the following two cases holds.

(a) r has a unique right inverse x and x is also a left inverse of r.

(b) r has infinitely many right inverses and no left inverse.

<u>Proof.</u> Assume first that r has a left inverse y. Then
$$y = y1 = y(rx) = (yr)x = 1x = x$$
and so $x=y$ is also a left inverse of r. Moreover, if x' is a right inverse of r, then
$$x' = 1x' = (xr)x' = x(rx') = x1 = x,$$
and so we are in case (a).

Assume now that r has no left inverse. Consider the elements

$$x_n = x + (1 - xr) r^n$$

for $n \geq 0$. Notice that

$$\begin{aligned} rx_n &= r(x + (1 - xr) r^n) = rx + (r - (rx)r) r^n \\ &= 1 + (r - r) r^n = 1 \end{aligned}$$

and so x_n is a right inverse of r for every n. Let $n > m$ and assume to a contradiction that $x_n = x_m$. Then

$$\begin{aligned} x_n = x_m &\Rightarrow x + (1-xr) r^n = x + (1-xr) r^m \Longrightarrow (1-xr) r^n = (1-xr) r^m \\ &\Rightarrow (1-xr) r^{n-m} r^m x^m = (1-xr) r^m x^m \Longrightarrow (1-xr) r^{n-m} = 1 - xr \\ &\Rightarrow (1-xr) r^{n-m} + xr = 1 \Longrightarrow ((1-xr) r^{n-m-1} + x) r = 1, \end{aligned}$$

where we used $r^m x^m = \overbrace{r \cdots r}^{m \text{ times}} \overbrace{x \cdots x}^{m \text{ times}} = \overbrace{r \cdots r}^{m-1 \text{ times}} \overset{1}{\overset{\parallel}{(rx)}} \overbrace{x \cdots x}^{m-1 \text{ times}} = r^{m-1} x^{m-1} = \cdots = 1$.

But $((1-xr) r^{n-m-1} + x) r = 1$ contradicts the assumption that r has no left inverse. Hence $x_n \neq x_m$ and so we are in case (b). $\square$

Proposition 2.20. The following are equivalent.

(a) R is an integral domain.

(b) The left cancellation property holds in R, that is if $r, s, t \in R$, $r \neq 0$ and $rs = rt$ holds, then $s = t$.

(c) The left cancellation property holds in R, that is if $r, s, t \in R$, $r \neq 0$ and $sr = tr$ holds, then $s = t$.

Proof. Exercise.